

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005 年 7 月 21 日 (21.07.2005)

PCT

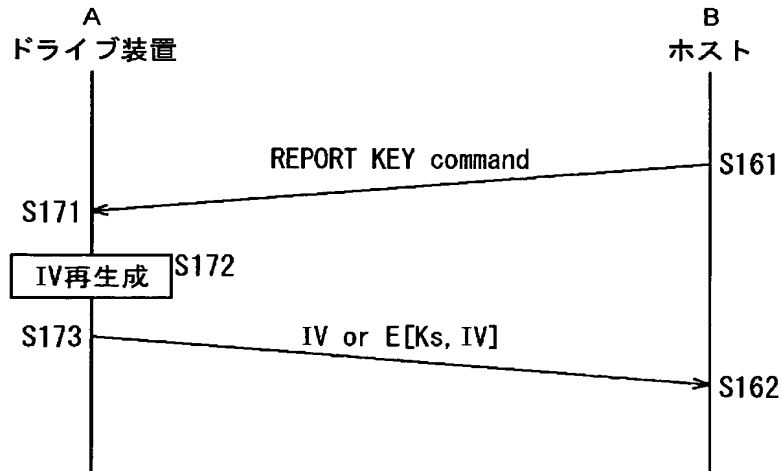
(10) 国際公開番号
WO 2005/067198 A1

- (51) 国際特許分類⁷: H04L 9/08, 9/16, G06F 12/14, G11B 20/10
- (21) 国際出願番号: PCT/JP2005/000061
- (22) 国際出願日: 2005 年 1 月 6 日 (06.01.2005)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2004-004798 2004 年 1 月 9 日 (09.01.2004) JP
特願2004-122524 2004 年 4 月 19 日 (19.04.2004) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 木谷 聡 (KITANI, Satoshi) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒1600023 東京都新宿区西新宿 7 丁目 1 1 番 1 8 号 7 1 1 ビルディング 4 階 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE

(54) 発明の名称: 情報処理装置



A DRIVE DEVICE
B HOST
S172 IV REPRODUCTION

(57) Abstract: There are provided an information processing device and method, program, and recording medium capable of transmitting/receiving data with a high security. A host is connected to a drive device by a predetermined bus, via which data is transmitted and received. The host periodically requests the drive device to issue an initial vector IV used for encryption and decryption of data transmitted and received via the bus. When the drive device has received the request, it generates the initial vector IV and supplies it to the host. If such a process is not performed periodically, the drive device stops data output to the host. The present invention can be applied to a personal computer having a drive device for reproducing data recorded on a recording medium.

(57) 要約: 本発明は、データの授受をセキュリティを高めた状態で行えるようにする情報処理装置および方法、プログラム、並びに記録媒体に関する。ホストとドライブ装置は、所定のバス

[続葉有]



SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR),

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

で接続されており、そのバスを介してデータの授受を行う。ホストは、ドライブ装置に対して、バス上を介して授受されるデータを暗号化および復号の際に用いられる初期ベクトルI Vの発行の要求を定期的に行う。ドライブ装置は、要求があったとき、初期ベクトルI Vを生成しホストに供給する。このような処理が定期的に行われなければ、ドライブ装置は、ホストに対するデータの出力を停止する。本発明は、記録媒体に記録されているデータを再生するドライブ装置を有するパーソナルコンピュータに適用することが可能である。